REMARKS/ARGUMENTS

This Response to Office Action is filed within six months of the mailing date of the Office Action from the Examiner mailed March 16, 2007. Reconsideration and withdrawal of the rejections set forth in the Office Action is respectfully requested. Claims 49 and 50 are new. Claim 42 has been cancelled. Claims 1-3, 10-12, 19, 25, 35-37, 40-41, 43-50 remain pending in the application.

THE PRIOR ART

The Examiner has rejected all pending claims under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,453,334 (Vinson et al.).

Vinson et al. describes in Column 2, lines 29-42:

> The present invention provides a method and apparatus for allowing a remotely-located computer program or data to be accessed on a local computer in such a way as to severely limit the possibility of said program or data being indiscriminately copied and propagated, plus providing time limits on the access to said program or data. A persistent caching scheme improves performance of subsequent accesses.
>
> A core component of the present invention is a network file system driver that simulates a local drive, but only allows access to that drive to designated computer processes. Process ID's are used to limit access to the program and/or data. A client program referred to as the client-agent accomplishes control of the network file system driver.

Vinson et al. disclose limiting access for three reasons, "the type of access being requested ..., the process ID of the process attempting the access, and optionally the path specified in the request for those request containing paths." (Col. 14, lns. 7-12). Vinson et al. describe limiting access based on the "the type of access" as

denying "any type of request that attempts to modify the content of the virtual drive." (Col. 14, 22-23) Vinson et al. describe limiting access based on the path specified as limiting access to certain directories by comparing the process ID of the requesting process to values stored in a "program descriptor block". (Col. 14, lns. 33-36).

Notably, Vinson et al. do not disclose granting or denying access based on the history of previous access requests by the process. Rather, Vinson et al. describe limiting access for the reasons listed above.

Additionally, Vinson et al. do not disclose granting or denying access based on whether the requested software file is a critical section requiring protection from piracy. Rather, Vinson et al. disclose allowing directory access to be limited by process ID, and do not disclose denying based on a specific section of the program or on the criticalness of the section.

Vinson et al. further describe a "deathwatch thread is to detect when the newly created process exits, so that the primary client-agent can perform any clean up associated with the process exiting." (Col. 8, lns. 17-20). The deathwatch thread waits for one of three events "the demise of the watched process, a timeout when the time allowed for the process to access the program expires ... , or the e_ShutdownClientAgent event becomes signaled." (Col. 8, lns. 22-26).

Notably, a deathwatch thread does not monitor, grant, or deny file access requests. Rather, the deathwatch thread performs certain cleaning tasks when a process is ended, but does not do anything during the execution of the process.

The examiner asserts:

> A deathwatch thread waits for a timeout when the time allowed for the process to access the program expires (Col. 8, lines 22-25), which meets the limitations of wherein said network file system ***examines said requests***, and either ***grants or denies each of said requests depending on whether the***

> ***request is justifiable from a security perspective*** by using information such as ***the history of previous access*** by the streaming enabled process (emphasis added).

Notably, a deathwatch thread does not examine filesystem requests and in fact has nothing to do with file system access requests. Vinson et al. describes the deathwatch thread as waiting for three events as described above. Because the deathwatch thread does not monitor filesystem requests and has no control over these filesystem requests, it is unable to grant or deny requests as the examiner asserts. Additionally, the deathwatch thread is not described as being used for security purposes. Furthermore, because the deathwatch thread does not track filesystem requests, and in fact has nothing to do with filesystem requests, it is unable to use the history of previous access requests.

THE PRIOR ART DISTINGUISHED

Independent Claims

Claim 1

The Examiner has failed to make a prima facie case for claim 1. Claim 1 includes the language:

> said network filesystem examines said requests, and either grants or denies each of said requests depending on whether the request is justifiable from a security perspective by using information that includes: ***the section of the targeted streaming software file being requested*** (emphasis added).

The Examiner has not asserted that Vinson et al. disclose granting or denying a request based on "the section of the targeted streaming software file being requested". The applicants respectfully assert that Vinson et al. apparently do not teach this language.

Claim 10

The Examiner has failed to make a prima facie case for claim 10. Claim 10 includes the language:

> said network filesystem examines each of said requests, and either grants or denies each of said requests depending on whether the request is justifiable from a security perspective by using information that includes, but is not limited to: the nature of the originating streaming-enabled process, ***the history of previous access by the streaming-enabled process***, and/or ***the section of the targeted file streaming application program being requested*** (emphasis added).

The Examiner has not asserted that Vinson et al. disclose granting or denying a request based on "the section of the targeted streaming software file being requested". The applicants respectfully assert that Vinson et al. apparently do not teach this language. Additionally, Vinson et al. do not describe a component which determines whether to grant an access based on the history of previous requests.

Claim 19

Claim 19 includes the language:

> said filesystem examines said requests, and either grants or denies each of said requests depending on whether the request is justifiable from a security perspective by using information that includes, but is not limited to: the nature of the originating streaming enabled process, ***the history of previous access by the streaming enabled process***, and/or ***the section of the targeted streaming software file being requested*** (emphasis added).

The Examiner has not asserted that Vinson et al. disclose granting or denying a request based on "the section of the targeted streaming software file being requested". The applicants respectfully assert that Vinson et al. apparently do not

teach this language. Additionally, Vinson et al. do not describe a component which determines whether to grant an access based on the history of previous requests.

Claim 25

Claim 25 includes the language:

> said filesystem examines each of said requests, and either grants or denies each of said requests depending on whether the request is justifiable from a security perspective by using information that includes, but is not limited to: the nature of the originating streaming enabled process, ***the history of previous access by the streaming enabled process***, and/or ***the section of the targeted streaming software file being requested*** (emphasis added).

The Examiner has not asserted that Vinson et al. disclose granting or denying a request based on "the section of the targeted streaming software file being requested". The applicants respectfully assert that Vinson et al. apparently do not teach this language. Additionally, Vinson et al. do not describe a component which determines whether to grant an access based on the history of previous requests.

Claim 35

Claim 35 includes the language:

> said processing device comprises a component that determines whether to grant requests for access to said streaming software files based on: whether an originating process that is making said requests for access is a trusted process, whether a ***history of previous requests*** for access made by said originating process ***exhibits a pre-determined pattern of piracy***, and whether a section of said streaming software files that is being requested is ***a critical section that requires protection from piracy***. (emphasis added).

Vinson et al. do not describe a component which determines whether to grant an access based on the history of previous requests. Vincent et al. do not describe using a pre-determined pattern of piracy. Vincent et al. do not describe a component which determines whether to grant access based on whether a critical section of streaming software files that requires protection from piracy is being requested. For any one of these reasons, claim 35 is allowable over the cited reference.

Claim 36

Claim 36 includes the language:

> said processing means includes a determination means for determining whether to grant requests for access to said streaming software files based on: whether an originating process that is making said requests for access is a trusted process, ***whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy***, and whether ***a section of said streaming software files that is being requested is a critical section*** that requires protection from piracy (emphasis added).

Vinson et al. do not describe a processing means which determines whether to grant an access based on the history of previous requests. Vincent et al. do not describe using a pre-determined pattern of piracy. Vincent et al. do not describe a processing means which determines whether to grant access if a critical section of streaming software files that requires protection from piracy is being requested. For any one of these reasons, claim 36 is allowable over the cited reference.

Claim 37

Claim 37 includes the language:

> said filtering means includes an evaluation means for evaluating: an originating process that is making said requests for access, ***a history of previous requests for access made by said originating process***, and ***a section of said streaming software application program files that is being requested*** (emphasis added).

Vinson et al. do not describe filtering accesses based on the history of previous requests. Vincent et al. do not describe filtering accesses based on the section of streaming software application program files. For any one of these reasons, claim 37 is allowable over the cited reference.

Claim 40

Claim 40 includes the language:

> determining whether an originating process that is making said requests for access is a trusted process, whether ***a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy***, and whether ***a section of said streaming software files that is being requested is a critical section that requires protection from piracy*** (emphasis added).

Vinson et al. do not describe determining whether to grant an access based on the history of previous requests. Vincent et al. do not describe using a pre-determined pattern of piracy. Vincent et al. do not describe determined whether to grant access based on whether a critical section of streaming software files that requires protection from piracy is being requested. For any one of these reasons, claim 40 is allowable over the cited reference.

Claim 41

Claim 41 includes the language:

> a means for determining whether said requests can be granted based on whether an originating process that is making said requests for access is a trusted process, whether ***a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy***, and whether a ***section of said streaming software files that is being requested is a critical section that requires protection from piracy*** (emphasis added).

Vinson et al. do not describe a means for determining whether to grant an access based on the history of previous requests. Vincent et al. do not describe using a pre-determined pattern of piracy. Vincent et al. do not describe means for determining whether to grant access based on whether a critical section of streaming software files that requires protection from piracy is being requested. For any one of these reasons, claim 41 is allowable over the cited reference.

Claim 43

Claim 43 includes the language:

> determining if a ***history of previous requests for access*** made by said computer process lacks ***a pre-determined pattern of piracy*** (emphasis added).

Vinson et al. do not describe a component which determines whether to grant an access based on the history of previous requests. Vinson et al. do not describe anything related to a pre-determined pattern of piracy. For any one of these reasons, claim 43 is allowable over the cited reference.

Claim 44

Claim 44 includes the language:

> determining if said section that is being requested ***is a non-critical section*** (emphasis added).

Vinson et al. do not teach a component which determines whether to grant an access based on whether the access if for a critical section that requires protection from piracy. For at least this reason, claim 44 is allowable over the cited reference.

Dependent Claims

Claims depending from any of the above-described independent claims are allowable at least for depending from an allowable base claim, and potentially for other reasons.

New Claims

Claims 49 and 50, which depend from claim 1, are allowable at least for depending from an allowable base claim and potentially for other reasons. For example, claim 50 includes the language:

> said network file system examines said requests, and either grants or denies each of said requests depending on whether the request is justifiable from a security perspective by using information that includes ***the history of previous access*** by the streaming enabled process (emphasis added).

Vinson et al. do not teach a component which determines whether to grant an access based on the history of previous requests. For at least this additional reason, claim 50 is allowable over the cited reference.

CONCLUSION

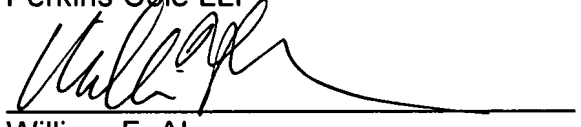
In view of the foregoing, Applicants submit that all the claims pending in the application patentably define over the prior art. The Applicants respectfully requests the Examiner withdraw rejections of all claims. A Notice of Allowance is therefore respectfully requested.

The applicants note that, due to the nature of the amendments, the Examiner should not need to perform any additional search. Accordingly, the applicants respectfully request that the amendments be entered.

If extra fees are due, please charge our Deposit Account No. 50-2207 from which the undersigned is authorized to draw.

If in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is encouraged to call the undersigned at (650) 838-4305.

Respectfully submitted,
Perkins Coie LLP



Date: May 10, 2007

William F. Ahmann
Reg. No. 52,548

Correspondence Address:
Customer No. 22918
Perkins Coie LLP
P.O. Box 2168
Menlo Park, California 94026
(650) 838-4300